STATE OF ALABAMA

Information Technology Standard

Standard 630-05S1_Rev B: Internet Content Management – Blocked Categories

1. INTRODUCTION:

Use of Internet resources for the purpose of accessing online games, Internet gambling sites, and viewing or downloading content inappropriate for official State business exposes the State and its data to risks including virus attacks, spyware and other malware threats, compromise of network systems and services, and potential legal issues. Accordingly, Internet content is managed to mitigate these risks.

2. OBJECTIVE:

Identify the categories of Internet content that are blocked in accordance with State IT Policy 630-05: Internet Content Management.

3. SCOPE:

This standard applies to all users (State of Alabama employees, contractors, vendors, and business partners) of any Internet-connected State-managed information systems.

4. REQUIREMENTS:

> *Policy: The State CIO has the authority to block certain categories of Internet content or specific web sites that present a threat to the security of State systems or are not deemed necessary for conducting official State business.*

By the authority of the State CIO, Internet users shall be denied access to the following content categories:

- Pornography/Nudity
- Gambling
- Online Games
- Spyware/Malware Sources and Effects

5. DEFINITIONS:

GAMBLING: Sites where a user can place a bet or participate in a betting pool, participate in a lottery, or receive information, assistance, recommendations, or training in such activities. Does not include sites that sell gambling-related products/machines or sites for offline casinos and hotels, unless they meet one of the above requirements.

ONLINE GAMES: Sites that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. Includes magazines dedicated to video games and sites that support or host online sweepstakes and giveaways.

SPYWARE EFFECTS: Sites to which spyware reports its findings or from which it alone downloads advertisements. Also includes sites that contain serious privacy issues, such as "phone home" sites to which software can connect and send user info; sites that make extensive use of tracking cookies without a posted privacy statement; and sites to which browser hijackers redirect users.

SPYWARE/MALWARE SOURCES: Sites which distribute spyware and other malware. This includes drive-by downloads; browser hijackers; dialers; intrusive advertising; any program which modifies your homepage, bookmarks, or security settings; and keyloggers. It also includes any software which bundles spyware as part of its offering.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 630-05: Internet Content Management

6.2 RELATED DOCUMENTS

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	5/23/2006	
Rev A	7/18/2007	Social Networking sites added
Rev B	5/11/2009	Social Networking sites removed